Estimation and Evaluation of the 1oo4-Architecture for Safety Related Systems

Josef Börcsök and Ali Hayek

Computer Architecture and System Programming, University of Kassel
Wilhelmshöher Allee 71, 34121,Kassel, Germany
j.boercsoek@uni-kassel.de, ali.hayek@uni-kassel.de

Abstract

In the standard IEC 61508 miscellaneous architectures for safety related systems are introduced. Depending on the required safety, reliability and availability levels several architectures such as 1oo2-, 2oo2-, 1oo3-, and 2oo3-architectures can be selected. In this paper, the concept and calculation of a novel architecture is presented. The 1oo4-architecture (one out of four) represents an advanced safety architecture, which is 3-failure safe. This means that at least one of the four channels have to work correctly in order to trigger the safety function. In order to classify the quality of the proposed architecture for safety related systems the PFD-value is calculated. Additionally, the Markov-model for a 1oo4-architecture is introduced and the MTTF-value for this architecture is calculated. The results are high safety and high reliability.

1. Introduction

Designing architectures for controlling safety related systems in all technical fields requires the consideration of several dependability aspects such as system complexity, functional safety, reliability and availability. The standard IEC 61508 presents several measures and design methodologies as well as system architectures, which treat these aspects [1]. Basically, the key factor of enhancing reliability, safety and availability of a given system is the use of system redundancy and diagnosis elements. However, nowadays almost only approved architectures with the lowermost redundancy are used in safety-related systems such as the 1oo2- and the 2oo3-architectures. There are various reasons for this: On one hand, higher redundancy leads to more complex systems with increasing system costs and power consumption, which are two key factors for designing such systems. On the other hand, the use of higher redundancy leads to more complex design issues such as synchronization and connectivity operations, which require additional components and highest verification and validation efforts. However, with the on-going miniaturization of semiconductor structures those reasons can be more and more neglected. On the one hand, a safety-related system with all needed components can be nowadays integrated into a single silicon chip, which reduces component count, system area, costs and power consumption. Additionally, due to the intra-chip communication highest synchronization and connectivity operations can be achieved. Furthermore, a high testability can be achieved due to various sophisticated EDA-tools for verification and validation of electronic chips. On the other hand, in the updated version of the standard IEC 61508 from 2010 guidelines for designing safety-related systems with on-chip redundancy are inserted [2].

On the basis of the presented arguments, a concept for the realization of a safety controller based on a quadruple redundancy (1oo4-architecture) for use in steer-by-wire applications has been presented in [3]. The benefits of this architecture are higher safety and higher reliability. In order to insert a higher availability to the proposed architecture a concept of degradability is introduced. Once a system failure is detected the failed system component will be excluded and the controller will be degraded to a 1oo3-architecture and so on to a 1oo2-architecture. However, this paper presents the proposed 1oo4-architecture as well as the calculation of the needed parameters for the evaluation of this architecture.

Section 2 briefly surveys the needed background on safety-related systems. In section 3 the proposed1oo4-architecture is introduced. In section 4 the calculation of the probability distribution is presented. For that a fault-tree analysis and the calculation of the average probability of failure on demand (PFD_{avg}) of the target architecture are introduced.

In section 5 the Markov model of the 1oo4-architecture is presented, from which the mean time of failure (MTTF) is deduced. Section VI finishes the paper with a conclusion and a short analysis about the presented architecture

2. Survey on Safety Related Systems

Today's controlling systems used for safety critical applications commonly consist of highly complex single components, implemented either as software or hardware. Hardware and software models have to be generated, evaluating aspects like reliability and safety of a complex system. The various functional, non-functional and safety-technical demands to the system along with common system characteristics lead to a list of system specific features. This contains:

- Reliability, availability and failure safe operation
- System integrity and data integrity
- Maintenance and system restoring

In order to have measurable parameters, the widely used parameters "mean time to failure" (MTTF) and "probability of failure on demand" (PFD) characterizes the quality of a faultless system. Combing all elements of a system in a safety architecture, the system can be classified with a defined safety level, the safety integrity level (SIL) [1].

On one hand, a system can be judged by its probability of a dangerous failure, i.e. an error occurs on the demand of a safety function and the system can no longer perform its safety function. This probability of failure is defined as "probability of failure on demand" (PFD). It has a dimension of 1 unit. A system's quality can be specified by defining its PFD value referred to its accuracy. The smaller this value is, the better the system is. The PFD value is calculated for a period of time called proof check interval T_1. After the maintenance of the system is carried out, it is assumed that it works without any failures. Judging and comparing systems is mostly specified by the PFD average value (PFD_{avg}) over a whole proof check interval.

On the other hand the MTTF-value can be calculated in order to evaluate system reliability. The MTTF-value is the mean time to the first failure under specified conditions. The MTTF-value is usually expressed in hours (h) or years (a).

The most known architectures are the 1oo2- and 2oo3-architectures, which are common for safety-related systems in industry. In order to meet all requirements for safety the 1oo2-architecture is sufficient. If an additional high availability is required a 2oo3-architecture has to be chosen. In order to take advantage of both systems in industry, a 2oo4-architecture has been developed [4, 5]. The 1oo4-architecture presented in the following achieves a higher safety and reliability level. The degradability concept enhances the proposed architecture with higher availability.

3. Description of the 1oo4-Architecture for Safety Related Systems

The 1oo4-architecture is a safety architecture that normally consists of four independent channels. The four channels are interlinked in such way that only one needs to resolve the safety function in order to carry out the safety function correctly.

A dangerous breakdown of the system is generated if three of the four channels have dangerous failures themselves. Each single channel contains an input circle, a safe processing unit and an output which is connected in series to the other channel outputs. In a fault-tree-analysis [6] it can be determined when a system can go into a dangerous non safety state:

- in four channels is a dangerous detectable failure which has a common cause
- in all four channels is a dangerous undetectable failure which has a common cause
- each of the four channels have a dangerous detectable or a dangerous undetectable failure which all have no common cause.

Theoretically, a 1oo4-architecture is immediately transferred from the operation state into the safe state if a dangerous failure arises. When a dangerous failure occurs then the faulty channel is switched off. Therefore, the 1oo4-architecture degrades to a 1oo3-architecture. In this new system it is still possible that another failure emerges. The system is in a defined state and it decides to go into the safe state. In a 1oo2-architcture one of the two channels has to work correctly. However, if there are two failures in each channel there is no possibility to switch the process into a safe state.

4. Calculation of Probability Distribution

In this section the mathematical and statistical calculations for the safety analysis of the 1oo4-architecture are presented. The safety analysis includes the analysis of failures and the performance of the system in relation to these failures. Especially the average probability of failure on demand is essential for the evaluation of the targeted SIL.

The basic approach can be applied to determine the PFD_{avg} -equation using the probability of failure function (*P(t)*) of a 1oo4-architecture. Therefore, the probability of failure $P_i(t)$ for a given element *i* is calculated using the following equation:

$$P_i(t) = 1 - R_i(t) \tag{1}$$

Where $R_i(t)$ is the reliability function of the element *i* given as follows:

$$R_i(t) = e^{-\lambda_i \cdot t} \tag{2}$$

Under the condition:

$$\lambda_i = \lambda_{D_i} + \lambda_{S_i} = const. \tag{3}$$

Where:

λ_i : is the overall failure rate of the i^{th} element.

λ_{S_i} : is the safe failure rate of the i^{th} element.

λ_{D_i} : is the dangerous failure rate of the i^{th} element.

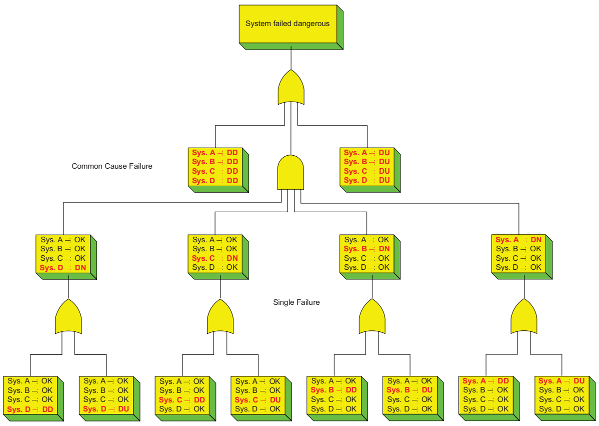

Fig. 1. Fault-tree-Diagram of the 1oo4-Architecture

In order to deduce the probability of failure for the 1oo4-architecture a hazards analysis is needed. The hazard analysis is a systematically method which is used to identify the dangers that face a given system. A popular technique that can be used for this purpose is the fault-tree-analysis. For the 1oo4-architecture the fault tree diagram is given in Fig. 1. According to this, the system can fail dangerously in the following cases:

- A dangerous detected (DD) failure occurs in all channels as a result of a common failure source.
- A dangerous undetected (DU) failure occurs in all channels as a result of common failure source.
- In each channel either a DD or DU failure occurs as a result of non-common failure source.

According to this, the total probability of failure is given by:

$$\begin{aligned} P_{1oo4}(t) &= P_{\text{single}} + P_{\text{common cause}} \\ &= P_1(t) \cdot P_2(t) \cdot P_3(t) \cdot P_4(t) \\ &\quad + P_{DUC}(t) + P_{DDC}(t) \end{aligned} \tag{4}$$

with $P_i(t)$ as the probability of failure for the ith system of a 1oo4-architecture. The probability of failure on demand is dependent from the time *t*, because as time increases, the PFD increases. The index DUC means a dangerous undetected common-cause-failure, whereas DDC accounts for a dangerous detected common-cause failure. In the following sections the calculation of each part of $P_{1oo4}(t)$ is introduced briefly.

4.1. Probability of Single Failures

If a 1oo4-architecture should fail with single failures, the system is within the condition that each channel has to have a dangerous failure. If the probability is calculated for this case, then the product is derived from the probability of failure of each channel and results in:

$$P_{\text{single}}(t) = P_1(t) \cdot P_2(t) \cdot P_3(t) \cdot P_4(t) \tag{5}$$

Where *P(t)* describes the probability of failure for the ith channel with the failure rate of

$$\lambda_i = \lambda_{D_i} \tag{6}$$

for a dangerous, single failure in channel *i* and the probability of failure

$$P_i(t) = 1 - e^{-\lambda_{Di} \cdot t} \tag{7}$$

If the equation (5) and (7) are used with the general applicable PFD_{avg} -equation, whereas $PFD_{avg}(T)$ is the probability of failure on demand until a given point in time T:

$$PFD_{avg}(T) = \frac{1}{T} \cdot \int_0^T P(t) \cdot dt \tag{8}$$

then the result is:

$$\begin{aligned} PFD_{avg,\ \text{single}}(T) = 1 &+ \frac{e^{-\lambda_{D1}T}-1}{\lambda_{D1}T} + \frac{e^{-\lambda_{D2}T}-1}{\lambda_{D2}T} + \\ &\frac{e^{-\lambda_{D3}T}-1}{\lambda_{D3}T} + \frac{e^{-\lambda_{D4}T}-1}{\lambda_{D4}T} \\ &- \frac{e^{-(\lambda_{D1}+\lambda_{D2})T}-1}{(\lambda_{D1}+\lambda_{D2})T} - \frac{e^{-(\lambda_{D1}+\lambda_{D3})T}-1}{(\lambda_{D1}+\lambda_{D3})T} \\ &- \frac{e^{-(\lambda_{D1}+\lambda_{D4})T}-1}{(\lambda_{D1}+\lambda_{D4})T} - \frac{e^{-(\lambda_{D2}+\lambda_{D3})T}-1}{(\lambda_{D2}+\lambda_{D3})T} \\ &- \frac{e^{-(\lambda_{D2}+\lambda_{D4})T}-1}{(\lambda_{D2}+\lambda_{D4})T} - \frac{e^{-(\lambda_{D3}+\lambda_{D4})T}-1}{(\lambda_{D3}+\lambda_{D4})T} \\ &+ \frac{e^{-(\lambda_{D1}+\lambda_{D2}+\lambda_{D3})T}-1}{(\lambda_{D1}+\lambda_{D2}+\lambda_{D3})T} \\ &+ \frac{e^{-(\lambda_{D1}+\lambda_{D2}+\lambda_{D4})T}-1}{(\lambda_{D1}+\lambda_{D2}+\lambda_{D4})T} \\ &+ \frac{e^{-(\lambda_{D1}+\lambda_{D3}+\lambda_{D4})T}-1}{(\lambda_{D1}+\lambda_{D3}+\lambda_{D4})T} \\ &+ \frac{e^{-(\lambda_{D2}+\lambda_{D3}+\lambda_{D4})T}-1}{(\lambda_{D2}+\lambda_{D3}+\lambda_{D4})T} \\ &- \frac{e^{-(\lambda_{D1}+\lambda_{D2}+\lambda_{D3}+\lambda_{D4})T}-1}{(\lambda_{D1}+\lambda_{D2}+\lambda_{D3}+\lambda_{D4})T} \end{aligned} \tag{9}$$

This function can be developed into a power series with the help of a Taylor series expansion (exactly MacLaurin series). The condition that the $PFD_{avg,\ \text{single}}(T)$ is a continuous function, which has a removable singularity at T = 0 and thus all derivations at this point exist can be proven, e.g. in [4, 7]. After some calculation, we get the simplified result:

$$PFD_{avg,\text{single}}(T) = \frac{\lambda_D{}^4 \cdot T^4}{5} \tag{10}$$

4.2. Probability of Common-Cause Failures

In this section the failure probability for dangerous undetectable and dangerous detectable common cause failures P_{DUC} and P_{DDC} are going to be calculated. Common cause failures are those failures that occur in all system channels at the same time and which have a common cause. When determining the PFD_{avg} this kind of failure is rated for a multi channel system through the β -factor. One distinguishes between the β -factor for dangerous undetectable failures, with the weight β, and the β -factor for dangerous detectable failures, with the weight β_D Calculating the common cause part of the total probability, the failure probabilities P_{DUC} and P_{DDC} have to be added:

$$P_\beta(t) = P_{DUC}(t) + P_{DDC}(t) \tag{11}$$

Analogue, these common cause failure probabilities can be derived for a 1oo1-architecture with $\lambda_{DU,1oo1} = \beta \cdot \lambda_{DU}$ and $\lambda_{DD,1oo1} = \beta_D \cdot \lambda_{DD}$. A random common cause failure represents a 1oo1 function block. Therefore, it is possible to apply the derived PFD_{avg} equation of the 1oo1-architecture for the calculation of probability of common cause failure, see [4]. The general solution for the probability failure results in:

$$PFD_{avg} = \frac{\lambda_D \cdot T}{2} \tag{12}$$

Since there are two common cause failure modes, $\lambda_{DUC} = \beta \cdot \lambda_{DU}$ and $\lambda_{DDC} = \beta_D \cdot \lambda_{DD}$, and with the two assumptions that:

- a dangerous undetected common cause failure occurs within the time period $T_1 + MTTR$ (T_1 means the proof time interval, MTTR means the mean time to repair) and
- a dangerous detected common cause failure occurs within the repair time MTTR,

the PFD_{avg} -value for common cause failures can be calculated as

$$PFD_{avg,\ \beta} = \frac{\beta \cdot \lambda_{DU}}{2}\left(T_1 + MTTR\right) + \frac{\beta_D \cdot \lambda_{DD}}{2} \cdot MTTR \tag{13}$$

The PFD_{avg} -equation of a 1oo4-architecture is taking into account the single failures, and the common cause failures.

Therefore, the total PFD_{avg} -equation can be given as follows:

$$PFD_{avg} = \frac{\lambda_D{}^4 \cdot T^4}{5} + \frac{\beta \cdot \lambda_{DU}}{2}\left(T_1 + MTTR\right) + \frac{\beta_D \cdot \lambda_{DD}}{2} \cdot MTTR \qquad (14)$$

The probability of a common cause failure is the same in a 1oo2-, 1oo3-, 2oo3-, 2oo4- and in a 1oo4-architecture. If the probability of a single failure in a 1oo4-architecture is compared with the probability of a 1oo2- or 1oo3-architecture, then the probability in a 1oo4-architecture is several dimensions smaller.

5. Reliability Analysis

4.2. Markov model of the 1oo4-Architecture

Markov models are stochastic models, which can be used for evaluating the safety and reliability of architectures. Basically, the Markov-model is a 1oo4-"Single-Board-System" accomplished with conventional calculation methods and represents the architecture using states and transitions. In the following the Markov model of the 1oo4-architecture given in Fig. 2 is described.

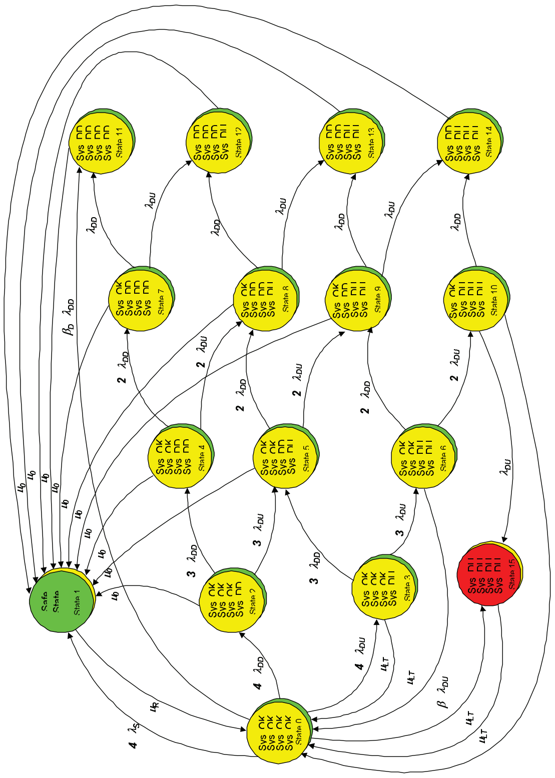

Fig. 2. Markov Model of the 1oo4-Architecture

Sate 0 represents the "non failure state" where all 4 channels are failure free. State 1 is the "safe state" in which the system devolves if a safe failure occurs. The transition rate from state 0 to state 1 is $4 \cdot \lambda_S$, because in each of the four channels is a safe failure possible. Furthermore, the 1oo4-architecture has fourteen different failure combinations. This leads to fourteen failure states. Due to page limitation a detailed explication is given on the basis of state 2 and state 3 only. Further states and transitions can be understood in a similar way.

In state 2 one of the four channels is operating with a failure. The occurring failure is dangerous and is not detected by the failure diagnostics. The transition rate between the states 0 and 2 has the value $4 \cdot \lambda_{DD}$, because in one of the four channels a dangerous detected failure can exist. The same can be applied for the transition from state 0 to state 3. Furthermore, from state 2 a transition takes place into state 4 respectively 5 if a detected or undetected failure occurs in the until then still failure-free channels. In the same way, from state 3 a transition takes place into state 5 respectively 6 if a detected or undetected failure occurs in the until then still failure-free channels (transition rates $3 \cdot \lambda_{DD}$ and $3 \cdot \lambda_{DU}$ respectively). However, no transition possibility exists for the system from state 3 into safe state 1 because the failure cannot be detected within the test interval $\tau_{Test} = 1/\mu_0$. The system can transfer from state 2 to state 0 with the transition rate μ_0. The system can only change from state 3 to state 0 again, where the system is failure free, after τ_{LT} if during the total lifetime of the system in state 3 no further failures occur. In praxis this means: After time τ_{LT} the total system is exchanged. Analogue, the system can propagate through other states.

Furthermore, following two cases can be distinguished while common cause failures occur in a 1oo4-architecture:

- The common cause failure leads to dangerous detected failures. Then a transition exists from state 0 directly into state 11. The transition rate is $\beta_D \cdot \lambda_{DD}$.
- The common cause failure leads to dangerous undetected failures. Then a transition exists from state 0 directly into state 15. The transition is $\beta \cdot \lambda_{DU}$.

4.2. MTTF-Calculation

From the Markov model described in the last section the MTTF value can be calculated. Therefore, a transition matrix P should be built (Probability of failure matrix). This transition matrix is a 16 x 16 matrix, because of the 16 different states. The P matrix is again the basis for the Q matrix. The elements of the Q matrix are composed of the respective probability densities, where the corresponding states meet the following criteria: "System operational" or "Non absorbing state".

An operational system is possible for a 1oo4-architecture in the states 0, 2, 3, 4, 5, 6, 7, 8, 9 and 10. The states 1, 11, 12, 13, 14 and 15 should not be considered during the MTTF calculation, as they are absorbing states. A state is called absorbing if it is impossible to leave this state (states have only outgoing transitions that are labeled with μ_0 and μ_{LT} transition rate). Therefore, the Q matrix has a 10 x 10 matrix form. For the considered Markov model we make the assumption of $\tau_{LT} = \infty$ is made and results in:

$$\mu_{LT} = \frac{1}{\tau_{LT}} = 0 \qquad (15)$$

Once the Q-matrix is built, the next step can be concerned, which is the calculation of the 10x10 M-matrix. The M-matrix is presented with the following formula:

$$\mathbf{I} - \mathbf{Q} = \mathbf{M} \cdot dt \qquad (16)$$

Afterwards the N-matrix will be calculated, which is the inverse matrix of the M-matrix. The N-matrix needs to be composed to derive the MTTF value of the system. The MTTF value describes the mean time between the occurrences of two failures. One assumes state 0 at the start time, i.e. the state in which the system operates failure free. After the inversion the elements of the new matrix represent time dependent values. One needs to sum up the first row of the N-matrix in order to derive the MTTF value of the system. The MTTF term of a 1oo4-system can be then calculated to the following form:

$$\begin{aligned}
MTTF_{1oo4} = {} & \frac{1}{A_1} + \frac{4 \cdot \lambda_{DD}}{A_1 \cdot A_2} + \frac{4 \cdot \lambda_{DU}}{A_1 \cdot A_3} + \\
& \frac{12 \cdot \lambda_{DD}^2}{A_1 \cdot A_2 \cdot A_4} + \frac{12 \cdot \lambda_{DU}^2}{A_1 \cdot A_3 \cdot A_6} + \frac{24 \cdot \lambda_{DD}^3}{A_1 \cdot A_2 \cdot A_4 \cdot A_7} + \\
& \frac{24 \cdot \lambda_{DU}^3}{A_1 \cdot A_3 \cdot A_6 \cdot A_{10}} + \frac{12 \cdot \lambda_{DD} \cdot \lambda_{DU} \cdot (A_2 + A_3)}{A_1 \cdot A_2 \cdot A_3 \cdot A_5} + \\
& \frac{24 \cdot \lambda^2{}_{DD} \cdot \lambda_{DU} \cdot (A_2 \cdot A_4 + A_3 \cdot A_4 + A_3 \cdot A_5)}{A_1 \cdot A_2 \cdot A_3 \cdot A_4 \cdot A_5 \cdot A_8} + \\
& \frac{24 \cdot \lambda_{DD} \cdot \lambda^2{}_{DU} \cdot (A_2 \cdot A_5 + A_2 \cdot A_6 + A_3 \cdot A_6)}{A_1 \cdot A_2 \cdot A_3 \cdot A_5 \cdot A_6 \cdot A_9}
\end{aligned} \qquad (17)$$

With

$$\begin{aligned}
A_1 &= 4 \cdot \lambda_S + 4 \cdot \lambda_{DD} + 4 \cdot \lambda_{DU} + \beta_D \cdot \lambda_{DD} + \beta \cdot \lambda_{DU} \\
A_2 &= \mu_0 + 3 \cdot \lambda_{DD} + 3 \cdot \lambda_{DU} \\
A_3 &= \mu_{LT} + 3 \cdot \lambda_{DD} + 3 \cdot \lambda_{DU} \\
A_4 &= \mu_0 + 2 \cdot \lambda_{DD} + 2 \cdot \lambda_{DU} \\
A_5 &= \mu_0 + 2 \cdot \lambda_{DD} + 2 \cdot \lambda_{DU} \\
A_6 &= \mu_{LT} + 2 \cdot \lambda_{DD} + 2 \cdot \lambda_{DU} \\
A_7 &= \mu_0 + \lambda_{DD} + \lambda_{DU} \\
A_8 &= \mu_0 + \lambda_{DD} + \lambda_{DU} \\
A_9 &= \mu_0 + \lambda_{DD} + \lambda_{DU} \\
A_{10} &= \mu_{LT} + \lambda_{DD} + \lambda_{DU}
\end{aligned} \qquad (18)$$

6. Conclusions

In this paper the 1oo4-architecture for safety-related systems was presented. The proposed architecture is targeted to use in automotive applications and can be targeted to be use in computer systems where higher safety, reliability and availability are required. As already mentioned in the introduction, today's technical systems will be more and more complex. One will no longer be able to provide appropriate safety in processes which has to be monitored. Future safety control must support him, either in recording and analyzing data, or in operation resulting from this. Advanced safety architectures like the introduced 1oo4-architecture have to be utilized in order to guarantee the required safety. The degradable 1oo4-architecture enhances the safety benefits of the 1oo2- and 1oo3-architecture and the availability of the 2oo3- and 2oo4-architecture: simultaneously a higher availability and a higher safety than today's systems. While the probability of a common cause failure is equal in all three system models, the probability of a single failure in a 1oo4-architecture is several dimensions smaller than in a 1oo3- or 2oo4-architecture as shown in Fig.3. Furthermore, one can see that the 1oo4-architecture provides a better MTTF-value that all established safety architectures. Due to the degradable concept the 1oo4-architecture also offers a high availability.

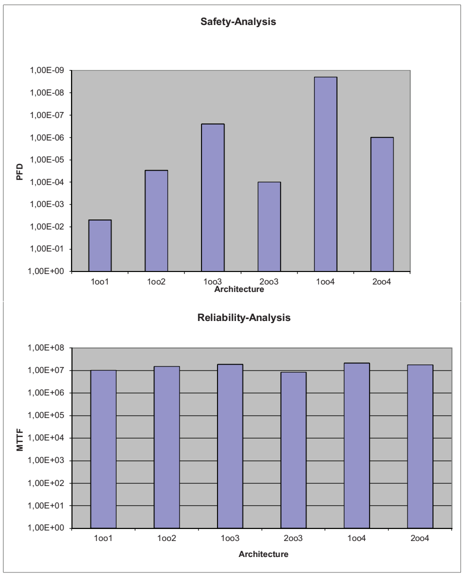

Fig. 3. Evaluation of the 1oo4-Architecture

7. References

[1] *IEC Commission, Functional safety of electrical/electronic/programmable electronic safety-related systems*, IEC 61508, part 1–7, CENELEC, Geneva, Switzerland, 2001.

[2] *IEC Commission, Functional safety of electrical/electronic/programmable electronic safety-related systems*, IEC 61508 Ed. 2, part 1–7, CENELEC, Geneva, Switzerland, 2010.

[3] J. Börcsök, M. H. Schwarz, E. Ugljesa, P. Holub, A. Hayek, "High-Availability Controller Concept for Steering Systems: The Degradable Safety Controller", to be published in WSEAS conference, Tenerife, Spain, 2011.

[4] J. Börcsök, "Electronic Safety System, Hardware Concepts, Models and Calculation", Hüthig Verlag, Heidelberg, Germany, 2007.

[5] J. Börcsök, "Functional Safety: Basic Principles of Safety-Related Systems", Hüthig Verlag Heidelberg, Germany, 2007.

[6] W. E. Vesely et. al., "Fault Tree Handbook. Nuclear Regulatory Commission", NUREG–0492, http://www.nrc.gov/reading-rm/doc/collections/nuregs/staff/sr0492/sr0492.pdf, retrieved 11-10-2011.

[7] M. Al-Bokhaiti, "Design and Implementation of Multi-Processor-based Communication Architecture for Safety-Related Applications Using FPGA", M.S. Thesis, EECS, University of Kassel, Kassel, 2011.